Response to Reviewer #2

We thank the reviewer for the thorough reading of the manuscript and the multiple suggestions that we believe have helped us improve the manuscript. We are grateful that the reviewer finds our model "interesting and informative". The reviewer's two concerns are addressed in order below.

1. *Recent BGP redirection attacks were presented as the paper's main motivation, yet the rest of the paper has very little to do with BGP. BGP is not a simple distance based routing algorithm, it is a path vector protocol that allows expressing complex business policies. A BGP speaking network typically announces different routes to different neighbors depending on its business relationship with them as well as from where it has learnt the route in the first place. Longer routes are often preferred over shorter ones depending on how money flows between networks (i.e. business relationship). After reading the paper, I was left with a question about what the paper has actually achieved. In my opinion, the paper has presented an informative model for information monitoring in networks with shortest distance based routing. It would be great if the authors can elaborate on how the presented model can help mitigating/avoiding traffic redirection in BGP.*

We thank the reviewer for pointing out this miscommunication. We have deeply revised the abstract and the introduction to better communicate our motivation and contribution to the literature. The main motivation of this work is routing misdirection or distance frauds but not BGP *per se*. In this work we study a theoretical model for distance frauds in an abstract setting of distance-vector protocols, and aim to provide a starting point to investigate security issues of other complex routing protocols. We have updated the paper to emphasize this point as well as the connection to the literature of distance-vector protocols. As the reviewer suggests, to apply our model to BGP network one needs to incorporate path-vector protocols and business details, which will be an important and interesting topic for future studies.

2. The conclusion about compromising just 18 random nodes in the US AS graph can lead to intercepting of all traffic is an over stretch for a couple reasons. First, to make a statement about a real world topology one needs to simulate BGP and not a distance-based routing protocol as mentioned above. Second, how did you measure traffic? have you used an actual traffic matrix?

Great point. We acknowledge that this statement is potentially misleading and over stretching. We have made two changes accordingly. First, we explicitly point out that the underlying routing protocol is a distance-vector protocol. As discussed in the response above, the aim here is to illustrate the effects of different strategies on a real network topology. The result serves as a baseline or starting point to study more complex routing protocols, e.g., BGP.

Second, by “traffic” we simply meant the number of node pairs. An equivalent assumption is that traffic is uniformly random across the graph. However, we agree with the reviewer that the use of “traffic” here could be confusing and unrealistic. Therefore, we have clarified this in the relevant section of the paper and updated the conclusion with a detailed discussion. The heterogeneous pattern of real-world traffic also provides another variable to consider in designing colluding strategies, which will be a promising direction for future work.